REMARKS

This communication is responsive to the Examiner's Answer of January 10, 2008, with an amendment under CFR Rule 1.111 to reopen prosecution in reply to the Examiner.

The purpose of the instant amendment presents the claims as amended and responsive to the Examiner's new grounds for rejection. Claims 15, and 17-31 stand rejected under 35 USC 101 as non-statutory subject matter, and while Applicants' do not acquiesce and in fact wish to point out to Examiner that were this the case the Notani claim which has much less recited structure would also non-statutory; nonetheless Applicants' instant reply amendment is primarily to provide clarification and present the pending claims, as amended, for reconsideration and allowance of all pending claims 15, 17-34 and 37.

A. Overview of the Invention

The present invention provides for a virtual private supply chain and viewing supply chain data using, for example, a generic Internet based viewing engine. Furthermore, the present invention facilitates achieving supply chain transparency, which enables enterprises to securely share order and inventory information among trading partners.

A virtual private supply chain (VPSC) is provided to facilitate collaborative, real-time exchange of supply chain data between multiple enterprises, which in turn facilitates reducing complexity and/or delays in a supply chain processing. A VPSC is a conduit through which supply chain data can flow in a timely, secure, consistent manner. Rather than a supply chain member having to maintain possibly distinct protocols, paperwork and records for communication with other members of a supply chain, by depositing selected data into a central supply chain data store, a supply chain member can maintain one protocol for communication with the central data store, thereby reducing complexity and/or delays in supply chain processing. The data to be deposited into the central data store may include purchase order information, sales order information, warehouse order

information, shipment information and inventory information. As inventory moves across a multi-enterprise supply chain, the present invention facilitates enterprises viewing information relevant to the deposited items and the inventory to which they relate, regardless of the source of information. Specification, page 12, lines 5-20.

1. Supply chain data store

Figure 4 illustrates a system 400 for providing a virtual private supply chain, which includes a common supply chain data store 430 into which one or more supply chain members 420_1 through 420_N deposit supply chain information (e.g. inventory positions, production capacity, purchase orders, sales orders, warehouse orders, etc.). Data may be extracted (e.g. pushed , pulled) from the supply chain members and placed into the common supply chain data store 430, and thereafter the common supply chain data store 430 and/ore related processes do not need to reach through security measures (e.g. firewalls) associated with the individual supply chain member data stores seeking data. This extraction of data may occur at any desired time including, but not limited to, on a periodic basis, on a manual trigger and on a data update trigger. The common supply chain data store 430 and/or associated processes can transform the supply chain data, which may be in inconsistent formats, to one or more common formats based on one or more common schema. Furthermore, the common supply chain data store 430 and/or associated processes can validate the supply chain data before loading it into the common supply chain data store 430. Further still, the common supply chain data store 430 and/or associated processes can determine relationships between supply chain member data and can control or regulate access to such related data. Specification page 10, lines 8-29. A supply chain data store that stores supply chain data in one or more common schemas and which also stores metadata (data about data) is further described at various points in the specification (e.g. data store 430 of Figure 4, page 10 at line 8, data store 650 of Figure 6, page 13 at lines 26-31, step 1760 of Figure 17, page 31 at lines 22-23, step 1840 of Figure 18, page 32 at lines 15-22).

2. Data acceptor

Figure 6 illustrates an architecture 600 that may be employed in a VPSC that includes a hub with a central VPSC application 640. The hub 640 receives transmissions from supply chain members 610, 620 and 630, decodes the transmissions, and then deposits data in the data store 650. Thus, hub and central VPSC application 640 is one example of a data acceptor (step 1720 of Figure 17, page 31 at lines 4-8, step 1810 of

Figure 18, page 32 at lines 8-10) that receives one or more supply chain data items from one or more supply chain members for storage in the data store.

3. Data accessor

Figure 1 illustrates a system 100 that includes a data store 110 where data 112 and metadata 114 associated with the data 112 are stored. System 100 also includes a generic Internet based display engine 120 that facilitates providing a metadata driven display 130 that displays data pursuant to metadata concerning what data should be displayed and how that data should be displayed or formatted. Figure 11 shows an example of a layout 1100 for a user interface provided by the engine 120. See specification at pages 7-8 and pages 20-29. See also step 1780 of Figure 17, page 31, step 1860 of Figure 18, and page 32. Thus, the engine 120 provides one example of a data accessor that selectively presents one or more supply chain data items stored in the supply chain data store to one or more viewing supply chain members.

a data accessor (1780) **operable to selectively present one or more supply chain data items stored in the supply chain data store** (650) **to one or more viewing** (1100) **supply chain members** (610, 620, 630)**; and**

In Figure 17, step 1780 says: "Selectively permit access based on ownership of supply chain data and/or relationships." Figure 11, at 1100, illustrates the view that is presented to supply chain members. The view is described in the application from page 20, lines 15 to 26. Views are presented "selectively", for example, with respect to security – row level security, preventing supply chain member A from viewing a row of data relating to transactions between supply chain members B and C, for example; and "menu level" security, limiting what menus a particular user can see. See application, page 29, line 24 to page 30, line15.

a component (1770) **that establishes one or more relationships within the supply chain data store between a first supply chain data item originating from a first supply chain member and one or more second supply chain items originating from one or more second supply chain members.**

In Figure 17, step 1770 says: "Establish one or more relationships between supply chain data received from two or more supply chain members." See application, page 31, lines 24-26 where it says, in part: "For example, a purchase order from a first VPSC member may be related to two sales orders from two different VPSC members."

17. The virtual private supply chain of claim 15 where an ownership identifier is established (1720) **within the supply chain data store for one or more supply chain data items**.

In Figure 17, steps 1720 and 1780 say: "Establish an ownership identifier for the supply chain data" and "selectively permit access based on ownership of supply chain data and/or relationships." See page 31, lines 7-10 and 24-31.

31. A computer readable medium (640) **storing computer executable components of a virtual private supply chain comprising:**

Figure 6 illustrates a hub and spoke virtual private supply chain (VPSC) 600, having supply chain members 610, 620, 630 operating behind firewalls and communicating with a central hub and VPSC application 640, and having a data store 650 operatively connected to the hub. (Application, page 13, lines 20-27).

a data accepting component (1710) **operable to receive one or more supply chain data items from one or more supply chain members** (610, 620, 630)**;**

Figure 17 is a flow chart illustrating a method 1700 for processing data in a VPSC. (For a description of Figure 17, see application, page 31, line 1 to page 32, line 2) Step 1710 says: "Accept supply chain data from one or more supply chain members."

a supply chain data (650) **storing component operable to facilitate storing** (1760) **of one or more supply chain data items received from one or more supply chain members** (610, 620, 630)**;**

In Figure 17, step 1760 says: "Store the supply chain data in a supply chain data store."

a data accessing component (1780) **operable to selectively present one or more supply chain data items stored by the supply chain data storing component** (650) **to one or more viewing** (1100) **supply chain members** (610, 620, 630)**; and**

In Figure 17, step 1780 says: "Selectively permit access based on ownership of supply chain data and/or relationships." Figure 11, at 1100, illustrates the view that is presented to supply chain members. The view is described in the application from page 20, lines 15 to 26. Views are presented "selectively", for example, with respect to security – row level security, preventing supply chain member A from viewing a row of data relating to transactions between supply chain members B and C, for example; and "menu level" security, limiting what menus a particular user can see. See application, page 29, line 24 to page 30, line15.

a supply chain data storing component (1770) **operable to establish one or more relationships within the supply chain data store between a first supply chain data item originating from a first supply chain member and one or more second supply chain data items originating from one or more second supply chain members.**

In Figure 17, step 1770 says: "Establish one or more relationships between supply chain data received from two or more supply chain members." See application, page 31, lines 24-26 where it says, in part: "For example, a purchase order from a first VPSC member may be related to two sales orders from two different VPSC members."

32. A computer implemented method (1700) **for providing a virtual private supply chain between two or more supply chain members, the method comprising the following computer executable acts:**

Figure 17 presents a method 1700 for processing data in a virtual private supply chain or VPSC. See application, page 31, line1 to page 32, line 2.

centralizing supply chain data from a plurality of supply chain members (steps 1710 and 1760)**;**

Figure 17 is a flow chart illustrating a method 1700 for processing data in a VPSC. (For a description of Figure 17, see application, page 31, line 1 to page 32, line 2) Step 1710 says: "Accept supply chain data from one or more supply chain members." Step 1760 says: "Store the supply chain data in a supply chain data store."

conforming the supply chain data to one or more common schema (step 1740)**;**

In Figure 17, step 1740 says: "Transform the supply chain data to a common format." See application, page 31, lines 14-19 which say, in part: "For example, data formatted according to a proprietary vendor schema may be converted to conform with a VPSC schema. For example, data may be transformed according to one or more of the schema illustrated in Figures 12 through 16."

selectively permitting access to the conformed supply chain data based on row-level security applied to the conformed supply chain data (steps 1730 and 1780, and page 29, line 24-31)**; and**

In Figure 17, step 1730 says: "Establish access permissions for the supply chain data." Step 1780 says: "Selectively permit access based on ownership of supply chain data and/or relationships." Page 29, lines 24-31 read as follows: "Figure 15 is an example of a schema associated with VPSC security. … There are multiple enterprises involved in processing associated with the present invention and thus the present invention facilitates preventing users of one enterprise from seeing data from other enterprise[s]. The schema illustrates the entities that support supply chain

row level security .... Enterprises can grant access levels including, but not limited to full access or related data only access to other enterprises."

4. Relationships component

In the example of Figure 1, the data 112 is supply chain data and the metadata 114 includes metadata concerning query criteria, view headings, additional information links, view results, personalization parameters, display content, display layout, and display format.

For example, the common supply chain data store 430 of Figure 4 and/or associated processes can determine relationships between supply chain member data and control access to such related data. For example, a purchase order from a first supply chain member may be related to inventory position information from a second supply chain member and a sales order from that same second supply chain member. Thus, in addition to the first supply chain member being able to view the first member's own data stored in the common supply chain data store 430, the first supply chain member may also be able to view related data (e.g. inventory position, sales order, and shipping information) given proper access permissions by other members. Specification page 10 at lines 18-25.

Further, the VPSC application of hub 640 of Figure 6 may establish ownership identifiers for received data items, establish access permissions for the received data items, and establish relationships between received data items. Specification page 13 at lines 26-31. See also step 1770 of Figure 17, page 31, lines 24-28, step 1860 of Figure 18, page 32, lines 23-29.

Thus, the common supply chain data store 430 of Figure 4 and/or associated processes as well as the VPSC application of the hub 640 shown in Figure 6 provide an example of a component that establishes one or more relationships within the supply chain data store between a first supply chain data item originating from a first supply chain member and one or more second supply chain items originating from one or more second supply chain members, such as sales from the first member to the second members.

B. Rejection of Claims 15, 17-33 and 37 Under 35 U.S.C. 102(e)

In this Section B, all of the claims are grouped together. Applicants suggests to the Board that claim 15 is representative of all these claims for the purposes of this

appeal. In Section C which follows, the patentability of dependent claim 17 and independent claim 33, which each require the establishment of ownership identifiers in supply chain data items, is separately argued. In that section, claims 18-23, which are dependent upon claim 17, are grouped together with claims 17 and 33. In Section D, the patentability of independent claim 32, which requires that row level security be used to grant selective access to supply chain data, is separately argued.

Claims 15, 17-34 and 37 stand rejected under 35 U.S.C. 102(e) as being anticipated by Notani. It is respectfully submitted that this rejection should be withdrawn for at least the following reasons. Notani does not teach or suggest each and every limitation of applicants' claimed invention.

For a prior art reference to anticipate, 35 U.S.C. 102 requires that "each and every element as set forth in the claim is found, either expressively or inherently described,
in a single prior art reference." In *re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949,
1950 (Fed. Cir. 1999) (quoting *Verdegaal Bros., Inc. v. Union Oil Co.,* 814 F.2d 628,
631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)).

The subject invention relates to providing a framework for exchanging data in various formats between trading partners in a supply chain, storing the data with data relationships clearly identified, and making the data visible in a consistent manner across the supply chain. For instance, data from three trading partners in a supply chain can be stored in a data store and relationships between their data can be established. See Figure 6. A purchase order from the first trading partner can be related to a shipping confirmation from the second partner and a receipt confirmation from the third partner. By entering the purchase order number, shipping number, or receipt number, any of the three trading partners can view the data relating to this series of transactions. In particular, as recited in amended independent claim 15 (and similarly recited in independent claims 31-33, and 37), Appellants' claimed invention can *establish one or more relationships* ***within the supply chain data store*** *between a first supply chain data item originating from a first supply chain member and one or more second supply chain data items originating from one or more second supply chain members.*

Notani does not teach or suggest the aforementioned novel aspects of applicants' invention as recited in the subject claims. Notani teaches workflows that are used to manipulate data as it is transmitted between two trading partners. These workflows are code that are contained and run within a Global Collaboration Manager, which is outside of the data store. Notani is silent regarding establishing one or more relationships within the supply chain data store between a first supply chain data item originating from a first supply chain member and one or more second supply chain data items originating from one or more second supply chain members.

The Examiner asserts in the Office Action that a hub and spoke architecture facilitates establishing relationships of data items and therefore anticipates the novel features of the subject claims. However, a hub and spoke architecture merely facilitates exchange of data between hubs and spokes. It does not establish relationships between data items within a data store. Furthermore, it is not inherent that a system which establishes relationships between data items in a data store will also establish a relationship between a first supply chain data item originating from a first supply chain member and one or more second supply chain data items originating from one or more second supply chain members. This relationship must be explicitly established.

C. Rejection of Independent claim 33, Dependent Claim 17, and Also Claim 34 (Dependent Upon Claim 33) and Claims 18-23 (Dependent Upon Claim 17).

Furthermore, claim 17 recites ***an ownership identifier is established within the supply chain data store for one or more supply chain data items***. Claim 33 contains similar language. Applicants' claimed invention allows for a data item or a group of data items in the data store to be identified as belonging to an entity, such as a company or an enterprise. This allows for multiple entities to each have ownership interests in a portion of the data items contained within the data store.

The passages in the Natoni patent cited by the Examiner (column 9, lines 53-54 and column 10, line 53 to column 11, line 11) do not speak of ownership and ownership rights. And contrary to the Examiner's assertion made in the Office Action (page 4, lines 19-21), simply verifying "that a partner is who it claims to be, plus [the] ability to collect data grouped by partnership" is not equivalent to establishing ownership of data by means of an identifier and does not anticipate the claim.

Public key encryption, as taught by the Natoni patent, verifies access rights and also authenticates a transaction, thus insuring that the party trying to access the data has

the privilege to do so and also insuring that the accessing party is who he or she claims to be. But such access rights are not analogous nor equivalent to ownership rights. An owner has the ability to grant access rights, whereas a user with only access privileges does not have this right. Moreover, public key encryption is implemented at the communications layer, and not in a data store. Furthermore, the grouping of data is not the same as establishing ownership of the data. For example, a system may group data provided by a first entity and assign ownership of that data to a second entity. The ownership identifier must be explicitly established to satisfy the claim requirement. Therefore, Notani fails to teach or suggest that an ownership identifier should be established within the supply chain data store for one or more supply chain data items.

D. Rejection of Independent Claim 32

Independent claim 32 additionally calls for the establishment of "row level security" applied to the supply chain data. This means that when a control chain activity report is displayed, such as the one illustrated in Figure 11, with each row representing a different transaction typically between two (or more) supply chain members, claim 32 specifically requires the rows of data representing the individual transactions to each include some form of security code that indicates to whom that specific transaction record (or row) may be displayed and to whom it may not be displayed. In support of this, the application says:

> There are multiple enterprises involved in processing associated with the present invention and thus the present invention facilitates preventing users of one enterprise from seeing data from other enterprise[s]. The schema [associated with VPSC security and presented in Figure 15] illustrates the entities that support supply chain row level security …. Enterprises can grant access levels including, but not limited to full access or related data only access to other enterprises. …" (Application, page 29, lines 26-31)

With the supply chain transactions being executed between many different pairs and groups of supply chain members and then being retained in a central supply chain data store that all of the supply chain members may freely share and search through, this provision of security at the individually displayable line of data level permits the

members to search freely yet prevents them from seeing the confidential transaction information reflecting the activities of other members.

For example, supply chain member A can search the data base freely and display all the lines of data representing transactions between member A and member B and all transactions between member A and member C. But member A cannot display and will never see all the lines of data representing transactions between members B and C and not involving member A -- those transaction lines are protected by row level security that keeps them from being displayed by the member A. (Sales between B and C, both of whom may compete with A, are none of A's business.) Row level security thus gives A the freedom to search the supply chain data store freely, but A never sees the confidential transaction lines belonging to other members..

The Examiner asserts that Natoni teaches this in column 10, line 53 to column 11, line 11 and also in columns 9, lines 44-58, which are reproduced below for the Board's convenience:

> Security
>
> A further problem with collaboration is the challenge of providing comprehensive security. Before enterprises can collaborate effectively, the security issue needs to be addressed. There are many different facets to security in a collaborative contest. Any multi-enterprise collaborative framework should address all of these different facets. The requirements for a collaborative security framework can include that: data exchanged between two partners should only be seen by the two partners; data exchanged between two partners should be tamper-proof; an enterprise should be able to verify that a partner is who it claims to be; the framework should not introduce new security holes into a partner's network; and the framework should be relatively easy to set up and administer.
>
> ....
>
> The technological security framework is a portion of the security scheme. The other portion has to do with the design of the collaborations themselves. The framework should allow enterprises to easily attach permissibilities to various actions that other enterprises can perform on it. The global collaboration workspace can support a hierarchical permissibility model with individual permissibilities attached to different data elements in the hierarchy. In particular, it can support user-specific and spoke-specific read, write, take and subscribe permissibilities. Hence,

> enterprises can finely tune who can read what data, who can write what data, who can take what data, and who can subscribe to write-notifications on what data.
>
> A third element in the collaboration framework security strategy is the ability to partition data across various collaborative workspaces. In particular, the collaborative workspaces are split into an internal collaborative workspace and an external collaborative workspace. Only data that needs to be truly shared with partners is in the external collaborative workspace. The rest is in the internal collaborative workspace. The external collaborative workspace is designed to sit either outside the corporate firewall or in an Extranet or DMZ. The collaboration framework design does not require the external collaborative workspace to make connections through the corporate firewall into the Internet (although it could).

Note that the word "row" does not even appear in this passage, much less the phrase "row-level security."

In support of this rejection, the Examiner says:

> Note that the ability to separate data rows specific to a collaboration, and further to set security attributes on a per element basis reads on row-level security. (Final Rejection mailed 02/24/2006, page 8, lines 4-8)

But there is no mention in the Notani patent of separating "data rows" – the phrase "data rows" does not appear in the text of the Natoni patent at any point – there is simply no occurrence of the word "row" in this patent. There is mention of attaching "individual permissibilities" to "different data elements" in the second paragraph quoted above, but the phrase "data elements" is a generic phrase of broad scope that encompasses all types of data elements and sets, whereas the phrase "data rows" is a much more limiting and specific phrase, particularly when considered the context of the one-line-per-transaction display presented in Figure 11 of the present application. The Examiner has thus failed to find "selectively permitting access to the … supply chain data based on row-level security applied to the … supply chain data" anywhere in the Natoni patent

D. Conclusion

Accordingly, Appellants respectfully submit that Notani fails to teach or suggest all limitations of Appellants' invention as recited in independent claims 15, 31-33, and 37 and in dependent claim 17 (and in all the claims that depend from these claims), and thus fails to anticipate the subject claimed invention. Therefore, it is readily apparent that this rejection should be withdrawn and Applicants respectfully request reconsideration and allowance of pending claims 15, 17-34 and 37.

If the Examiner would like to discuss Applicant's invention prior to issuing a further action, the Examiner should feel free to contact the undersigned attorney.

In view of the foregoing, Applicants request consideration of and respectfully requests allowance of pending claims 15, 17-34 and 37.

Respectfully submitted,

/perry hoffman/

Perry Hoffman
Registration No. 37,150
PERRY HOFFMAN & ASSOCIATES, P.C.
P.O. BOX 1649
DEERFIELD, IL 60015
(847) 809-4285; (847) 607-0580 (FAX)

Attorney Docket No. 21-019 ITW 20557